Data and analytics (D&A) driven risk transformation for banks

February 2022

pwc

Table of contents

Introduction

The global financial crisis of 2007–08 was an event which had a significant impact on the overall view of risk management and regulation in the financial services (FS) industry. As a response to the crisis, the Basel Committee issued the 'Principles for Sound Liquidity Risk Management and Supervision' in September 2008, which was followed by the introduction of new capital and liquidity standards in the coming years. In December 2017, the Group of Central Bank Governors and Heads of Supervision, the Basel Committee's oversight body, endorsed the finalisation of Basel III reforms, thereby strengthening the three pillars established by Basel II.[1]

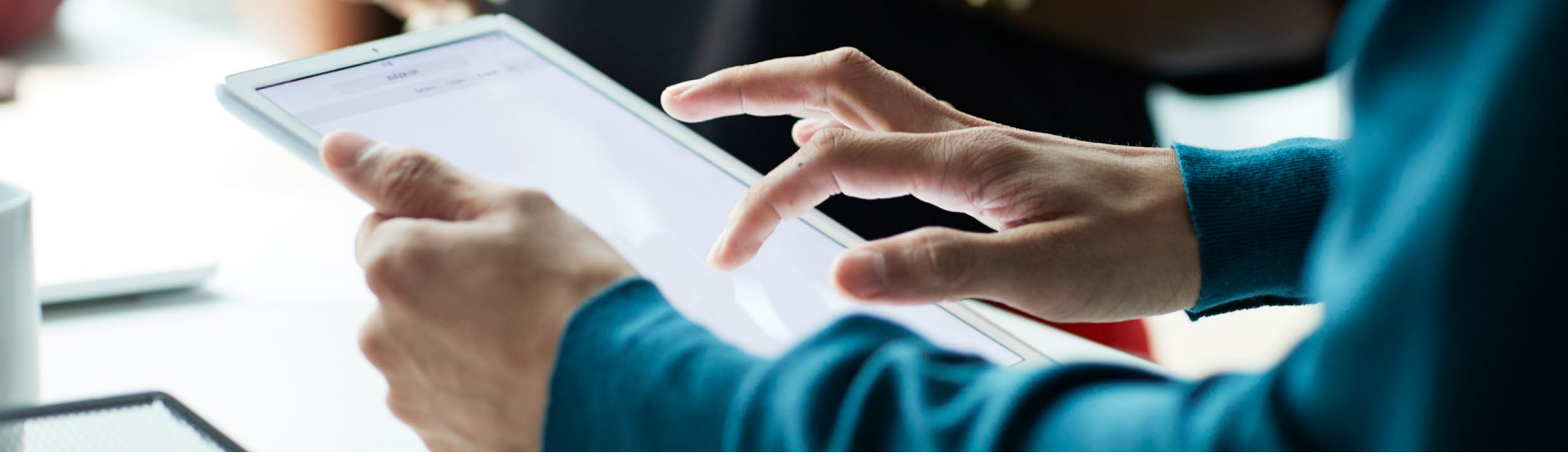
Global financial systems, which have been significantly impacted by the COVID-19 pandemic, will undergo their first major test after implementation of the reforms following the 2007–08 financial crisis. Measures taken to contain the spread of the virus have adversely impacted the smooth functioning of the global economy. While some organisations have been resilient and weathered the pandemic's effect by embracing new digital ways of working and generated positive sentiments in investors, others are still facing challenges. The pandemic's economic impact has also highlighted the importance of efficient operational risk management as the digitisation of operations and evolving business models might lead to the emergence of new risks. Efficient risk management in the financial sector has again taken centre stage amidst the pandemic induced challenges.

Regulators worldwide are continuously developing and implementing measures to enhance crisis management preparedness amongst financial institutions (FIs).

Implementation of the Basel III regulations will also increase focus on capital adequacy, asset quality, stable funding and liquidity management. Regulators expect FIs not only to react to but also identify any possible future stresses or uncertainties and act pre-emptively towards alleviating them.

In the coming years, we can expect tighter regulations, increased regulatory penalties and management sanctions on organisations for not taking preventive measures.

1 https://www.fsb.org/work-of-the-fsb/implementation-monitoring/monitoring-of-priority-areas/basel-iii/



The Reserve Bank of India (RBI) plans to review the existing Risk Based Supervision (RBS) models to make them more robust and capable of addressing emerging challenges. The central bank aims at building efficient governance, oversight and assurance functions. It also plans to review the existing CAMELS (capital adequacy, asset quality, management, earnings, liquidity, systems and controls) based supervisory approach for urban cooperative banks (UCBs) and non-banking financial companies (NBFCs) to build an efficient and forward-looking risk management culture. In the same spirit, the RBI has been moving away from the traditional provision computation based on losses that have already occurred to expected credit loss (ECL) based provisioning which considers future indicators and macroeconomic factors. This is in line with the International Financial Reporting Standards (IFRS 9).

The RBI Governor has repeatedly emphasised on the need of an efficient risk management culture in banks and NBFCs. He reiterated the same in RBI's annual report released in August 2020, stressing on the need of an effective and sophisticated risk management system which can identify risks and vulnerabilities well in advance and capture them in sync with the changes in the external environment and best practices.[2] In September 2021, the Deputy Governor highlighted the need of building a resilient financial system. He said that such a system should be able to deal with an entire range of shocks.[3]

The RBI's view on proactive risk management has strengthened in the light of systemic shocks such as Infrastructure Leasing and Financial Services (ILFS) defaulting on its debt obligations[4] and asset quality challenges at Yes Bank.[5] Hence, the central bank is moving towards efficiently managing risk using evolving technology solutions.

To prevent the sudden collapse of institutions during a period of economic stress or uncertainty, regulators are focusing on real-time internal monitoring of aggregate exposures and other risk parameters. Further, digital technologies powered by artificial intelligence (AI) and machine learning (ML) are increasing the scope and efficiency of risk management as well as regulatory capacity. For example, FIs are applying AI/ML models to identify patterns in high-volume transactions and flag off potential fraudulent scenarios such as trade spoofing and wash trading. The technology landscape in FIs is rapidly evolving with the rise of FinTech, InsurTech, RegTech and SupTech start-ups. Established players will have to compete as well as collaborate with these agile organisations and their technical prowess. Apart from digitisation, the recently introduced new norms for environmental, social and governance (ESG) disclosures will further increase scrutiny as well as enforcement and litigation risk. All these factors are contributing to the rising scope and frequency of risk measurement and regulatory compliance.

Hence, automating risk management and compliance activities, and making them cost effective, is now more important than ever. We expect to see widespread transformation in risk management in the FS industry in the next decade.

2 https://economictimes.indiatimes.com/industry/banking/finance/banking/risk-aversion-will-be-self-defeating-for-banks-rbi-governor-shaktikanta-das/articleshow/77778982.cms?from=mdr

3 https://www.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=20497

4 https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/0FSRDECEMBER20198C840246658946159CB3B94E8516F2EC.PDF

5 https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=49476

Need for risk transformation in the FS industry

Evolving risk and regulatory requirements

The pandemic has adversely affected most businesses in India, resulting in a potential increase in non-performing loans for banks and other FIs. This crisis has made it imperative for FIs to be more agile in recalibrating their risk profile to tide over such unforeseen circumstances. Technology-enabled risk transformation helps FIs to respond better to such changes through a robust risk data model and reporting framework.

As per the RBI's Systemic Risk Survey released in July 2021, most of the respondents expected a decline in the credit demand and deterioration in credit quality over the next three months due to the uncertainty caused by the second wave of the pandemic.[6] However, credit demand expanded across select 33 scheduled commercial banks (SCBs) between June–November 2021, with an increase in agricultural credit and slight decrease in micro, small and medium (MSME) credit.[7]

The RBI has been increasingly issuing a number of regulations every year since the global economic crisis of 2007–08. It has taken a firm stance against any form of non-compliance in the recent past. It imposed a cumulative penalty of INR 14.5 crore on 14 banks in July 2021.[8]

It is also developing its regulatory reporting and information infrastructure in the form of Public Credit Registry (PCR) and Central Information and Management Systems (CIMS). These measures have led to an increase in compliance costs for banks and other FIs, and they are prioritising the optimisation of regulatory and compliance processes.

Regulators are expecting FIs to submit more granular data, with data elements being added frequently. Each year, 20% of the data elements are estimated to be changed or redefined.[9] This necessitates the availability of agile technology infrastructure at an FI's back end, capable of handling huge volumes of data, having low latency, supporting standardisation and maintaining data integrity.

The increase in digital adoption has led to rising instances of financial fraud and crimes. This is expected to further accelerate the usage of advanced analytics techniques like pattern recognition, behavioural biometrics and AI-enabled predictive modelling for detecting fraud. As digital interactions between customers and banks for KYC-like processes increase, data governance has assumed greater significance due a huge volume of personally identifiable information (PII) available with banks. Cyber security has become a mandatory requirement for all FIs because of the ever-expanding digital footprint. In 2020, the average cost of data breach in India was INR 14 crore, a 9.38% increase compared to the previous year.[10] Banks and other FIs are prioritising the management of credentials and securing data, and any security breach is a reputational and financial risk to the institution.

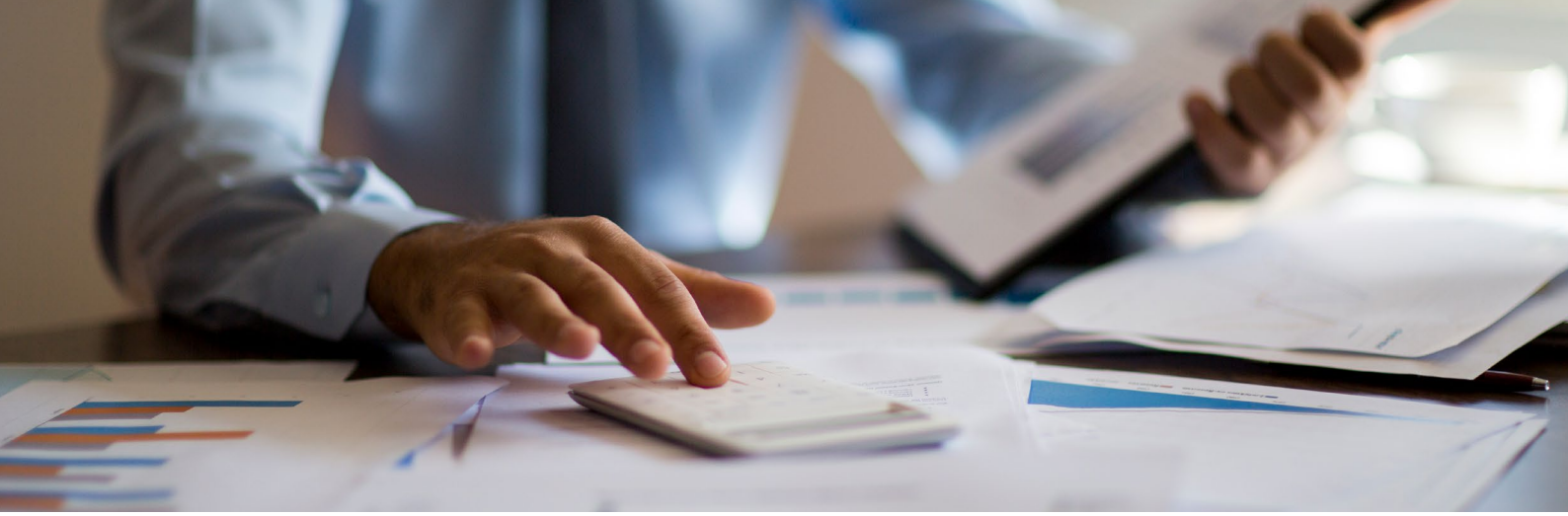
6 https://m.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1182

7 https://rbi.org.in/Scripts/Data_Sectoral_Deployment.aspx

8 https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=51863

9 https://www.wipro.com/banking/future-ready-regulatory-reporting/

10 https://www.ibm.com/blogs/digital-transformation/in-en/blog/6-reasons-why-businesses-need-regtech-more-than-ever/



The COVID-19 crisis has accentuated the importance of incorporating non-financial operational risks like ESG, pandemics and natural disasters, technology, cyber and business continuity into the enterprise-wide risk management framework. Compliance with ESG and related disclosures are also monitored by other regulators like the Task Force on Climate Related Financial Disclosures (TCFD).

This means that FIs needs to perform proactive credit assessment of high-risk industries and localities. They would need to tap into structured, unstructured and other data sources to gather information on non-financial risks and technology would be helpful in automating these data acquisition efforts. The firmwide data models need to be flexible enough to incorporate these data elements when required.

New and emerging types of risk

Financial risks like credit, liquidity and market risks have been a part of risk management frameworks in banks and other FIs for over 20 years now. Operational risk has gained traction in the last ten years.

In the recent past, newer risks have emerged in the wake of digital expansion, extensive data availability and the pandemic. Some of these emerging risks that are important to all stakeholders involved are highlighted below:

Emerging risks	
Risk category	**Mitigation description**
ESG	1. Reduce contribution to climate change through efficient use of renewable energy sources 2. Diversity and equity in the workplace 3. Healthy working conditions for employees 4. Transparent disclosure of information to all stakeholders 5. Incorporate non-credit ESG factors like identification and recalibration of high-risk industries, assessment of ESG factors in any new product launch and measurement of investment risks due to evolving ESG guidelines
Privacy	Continuous monitoring and upgradation of cyber security systems to prevent any kind of privacy attack
Credit	Build credit risk assessment models with adequate flexibility to absorb variations in risk profile as a result of extreme events like the COVID-19 pandemic

Our framework for D&A-driven risk transformation

PwC's framework for D&A driven risk transformation stands on three broad pillars, as described in the figure below:

Process and governance

- Operating model
- Standard operating procedure
- Risk and control logs
- Reconciliation
- Risk review and exception management
- Remediation

People and culture

- Risk data governance council
- Risk management policy
- Data stewards
- Data access, ownership and privacy
- Transparent communication to senior management and board

Data and reporting

- Master data management
- Business glossary and golden source for critical data elements
- Data lineage and traceability
- Data quality
- Data warehouse with comprehensive risk data model and marts
- Risk reporting and management dashboards

Pillar 1 – process and governance

The target operating model adopted by FS organisations should imbibe efficient risk management procedures correspondent to their business models and risk appetite. They should look at the entire spectrum of risks, i.e. both traditional and emerging risks, and develop policies around for accurately measuring and mitigating them.

Standard operating procedures (SOPs) for all the processes along with service level agreements (SLAs) and responsibilities should be clearly defined. SOPs should also cover fallback mechanisms which detail the exception scenarios and steps to manage them.

Data reconciliation reports should be generated at the intermediary layers of a data platform to ensure data quality. There should be well-defined SOPs for reconciliation activity which should cover the SLAs, accountable user groups and treatment of unreconciled entries.

Additionally, the risk-review process should be efficient with clear demarcation of roles and responsibilities of each individual in identifying, optimising and mitigating risk. The purpose of each risk report should also be validated periodically. Validations are required to ensure that relevant recipients receive reports within an agreed timeline. Exceptions identified as results of risk review should be transparently reported and the findings should be incorporated into the risk management procedures to make them more efficient. A central repository for risk and control logs along with possible remediations should be maintained for easy reference of stakeholders.

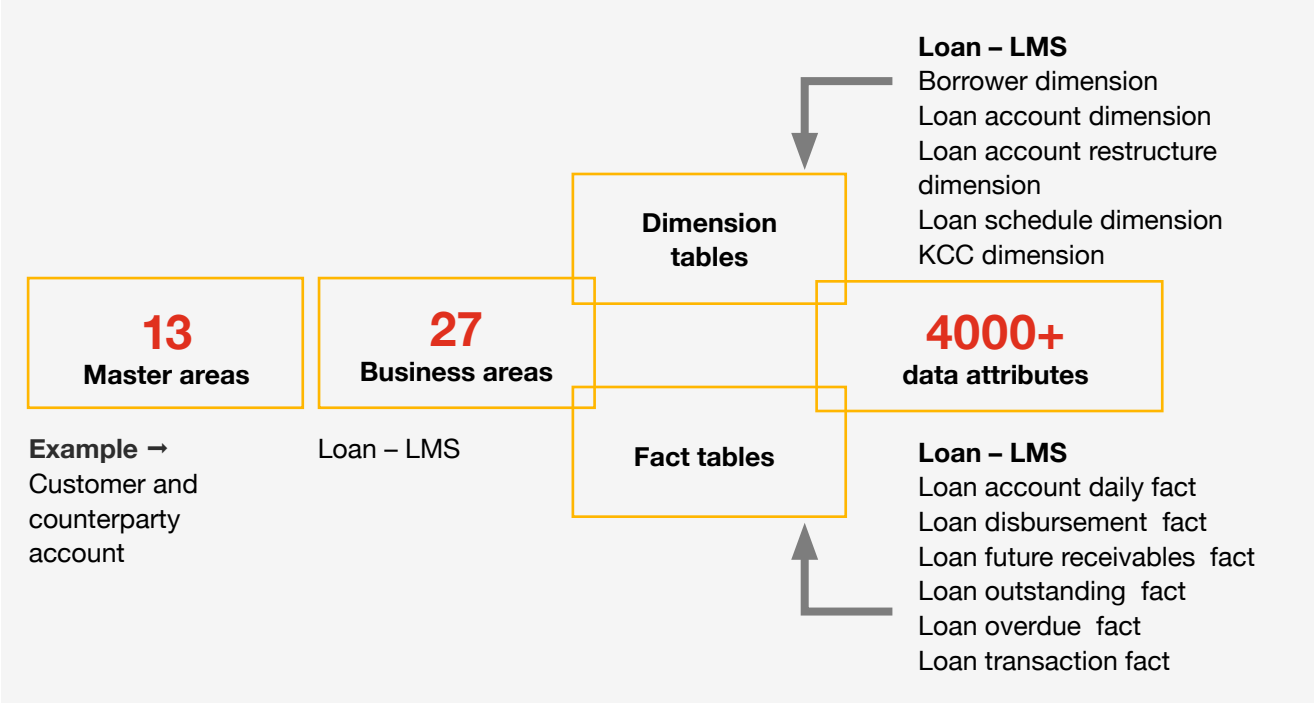
Pillar 2 – data and reporting

A comprehensive risk data model which acts as a single source of truth for all downstream risk use cases is critical to reduce latency in the availability of risk KPIs and eliminate key personnel dependency for making it available.

PwC's Risk Data Model covers the following subject areas. It is a continuous maturing and evolving model, and the below infographic covers its details, as of January 2022.

1. Credit underwriting and risk monitoring
2. Risk-based supervision mandate covering quantitative data points
3. Early-warning system and related analytics
4. Regulatory reporting and BASEL disclosures

The figure below details the functioning of the Risk Data Model:



- Data model caters to all the risk and regulatory areas covering – **credit underwriting and risk monitoring, risk-based supervision mandate, regulatory reporting under ADF/CIMS, early warning data points and Basel disclosures, including LCR, NSFR**
- The RBI indent main data set gets covered within the key subject areas of the data model – **GL level assets, liabilities, balance sheet, profitability, loan account level data, asset class, securitisation, restructuring, investments, liabilities, base data for key ratios computation, ECL, early warning liquidity indicators**
- Master areas would contain master tables such as **customer, product, account and channel masters**
- Business areas comprise **loans, derivatives, investment, deposits, trade, general ledger**, etc.
- Dimension tables contain attributes **describing the objects in a fact table**
- Fact table contains **measurements, metrics, and facts about a business process**, and daily and transactional facts are part of the model

An overview of the functional coverage of the Risk Data Model is given below:

Subject area	Credit underwriting and risk monitoring	Risk-based supervision mandate	Early warning system and related analytics	Regulatory reporting and Basel disclosures
KPIs	• Gross/net non-performing assets • Liquidity coverage ratio/ net stable funding ratio • PD, LGD and EAD • Bucket-wise cash flow	• Exposures across industry and product dimensions • Borrowings and deposits by maturity profile • PV01 and VaR of investments and derivatives	• Financial ratios • Capital requirements • Legal cases against organisation • Collateral performance	• Exposure and risk KPIs in returns like CRILC, RLC and SMA • Basel ratios like leverage ratio and CET ratio
Snapshot tables for reporting	Tables to cater to the requirement • Loans • NPA • Deposits • Investments • Asset Recovery	Tables to cater to the requirement • Customer and exposure • Investments and derivatives • Loans, deposits and borrowings	Tables to cater to the requirement • General ledger • Legal cases • Limits and collaterals	Tables to cater to the requirement • Customer and exposure • General ledger • Loans

A risk data model should be augmented with a master data management (MDM) framework to ensure uniformity, consistency and accountability of enterprise data. Standards for golden source of data, reference and risk data taxonomy should be defined.

A business glossary of critical risk data elements could be created to ensure consistent understanding across departments and regulations. The precision requirements of risk data elements in the data model should be created based on bank validation rules, testing or reconciliation processes, and earlier results of risk reporting.

Automated tool-based data lineage solutions should be deployed to establish traceability between reporting elements and source data. The accuracy of the insights provided by the risk models and dashboards relies heavily on the quality of incoming data. Data quality is a key consideration since data is obtained from disparate sources in an enterprise-wide risk management set-up. Individual business processes, which are a part of the overall risk management framework, should ensure the quality of the first level of data collected since they own the data. These systems should be capable of configuring business rules to maintain data quality.

Once the data warehouse risk management model is implemented using the Enterprise Risk Data Model, use case specific data marts could be created to enable faster access to data and insights.

In addition to building data marts, generating customised reports and developing dashboards can provide key insights and assist in decision making.

Pillar 3 – people and cultural impact

Along with data, infrastructure and process governance, people and organisational culture help in creating a robust risk-management framework. Employees need to adhere to risk principles and pointers as a part of their day-to-day operations. This requires an organisation to clearly define its risk management policy. For steering the risk data governance programme and enabling data quality and regulatory compliance, a risk data governance council should be established. The council's objectives should be to manage the availability, usability and integrity of risk data, and ensure effective data usage. An organisation's data policy should have distinct guidelines on which user groups should own and be provided access to particular types of data. Data privacy should be a key consideration in deciding data access and ownership. Organisations should also create 'data steward' roles for those who are responsible for overseeing data governance.

The senior management and the board along with the established council need to review and approve an FI's group risk data aggregation and risk reporting framework, and ensure that adequate resources are deployed.

Transparent communication with senior management and board on risk issues is paramount to maintaining a strong risk culture. The organisational culture should encourage employees to speak up, if required, on any risk that they foresee, without being apprehensive about undesirable consequences.

It is important for an organisation to treat risk as a strategic initiative for business rather than an overseeing control function.

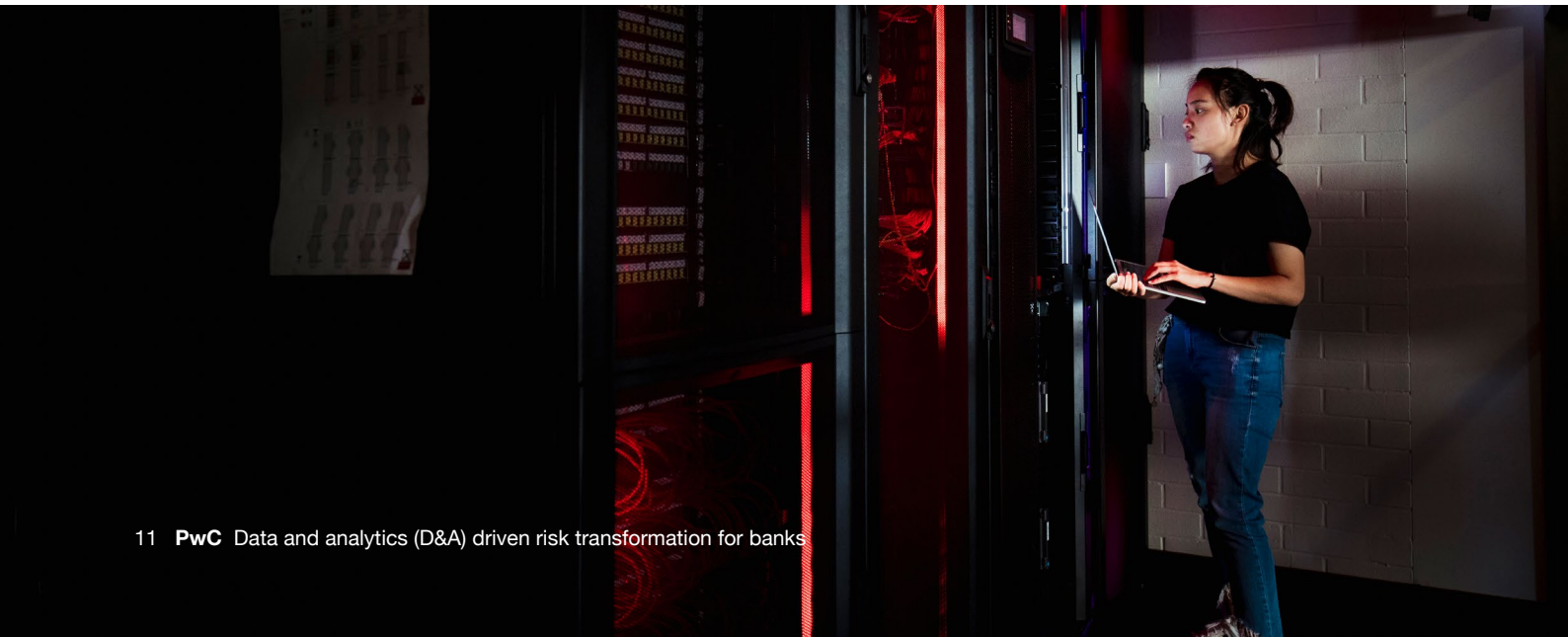
Additionally, D&A-driven risk transformation benefits FIs both in terms of cost and effort. In the absence of a centralised data platform, considerable efforts go into data consolidation and clean-up which can be otherwise spent on analysing and deriving business-critical insights. The efforts spent on manual data consolidation is directly proportional to cost as it requires the presence of a larger team for iterative operational and transactional tasks.

New technologies for risk identification and mitigation

New technologies could be employed to assess and measure risks as business models and ways of doing business have evolved amidst the disruption caused by the pandemic. They can be augmented with the framework described above to reinforce the risk management activities in an organisation.

A few examples of the new technologies adopted for risk management are given below:

Technology use cases in risk analytics transformation		
S.no.	**Functional use case**	**Technology**
1	Credit assessment models	AI/ML
2	Portfolio monitoring and early warning signals (EWS)	AI/ML
3	Transaction monitoring for frauds	AI/ML
4	Liquidity assessment models	AI/ML
5	Identification of optimal price points relative to market risk to maximise the returns	AI/ML
6	AML/KYC	Intelligent automation (IA)
7	Compliance related auditing	IA
8	Regulatory interpretation	NLP
9	Process regulatory and compliance updates from regulators	NLP
10	Use of unstructured data from data sources like regulatory websites, news, social media and public sources to mitigate newer risks related to compliance, customer satisfaction and brand perception	Big data, advanced analytics
11	Interactive and more engaging employee training on risk controls involving scenario simulations	Virtual reality (VR)/augmented reality (AR)



Conclusion

The economic outlook has undergone several changes in the past one-and-a-half years. A common risk and regulatory data platform can help FS organisations remove biases and be ready to adapt to the new normal. Such a platform will have the flexibility and scalability to identify new risks emerging from evolving business models and mitigating them can help build trust and deliver sustained outcomes. Risk monitoring would gradually move away from an event-based approach to a continuous monitoring process.

It is essential for organisations to optimally align people, processes and data to gain maximum benefits out of their transformation journey. Meticulous planning is required to ensure that the different elements of a risk and regulatory data platform are timely available and effective in aiding an organisation in achieving its vision. Post implementing a risk and regulatory data platform, an FS organisation can deploy additional advanced analytical tools to accurately measure 'known-known/known-unknown' risks, and predict and measure 'unknown-unknown' risks.

In addition to adhering to compliance, a common risk and regulatory data platform provides additional advantages such as:

01 A holistic view of business and associated risks at an organisation level

02 Enhanced management insights assisting formulation of product/channel/people strategy

03 Avoidance of ongoing tactical projects to plug reporting gaps resulting in cost benefits

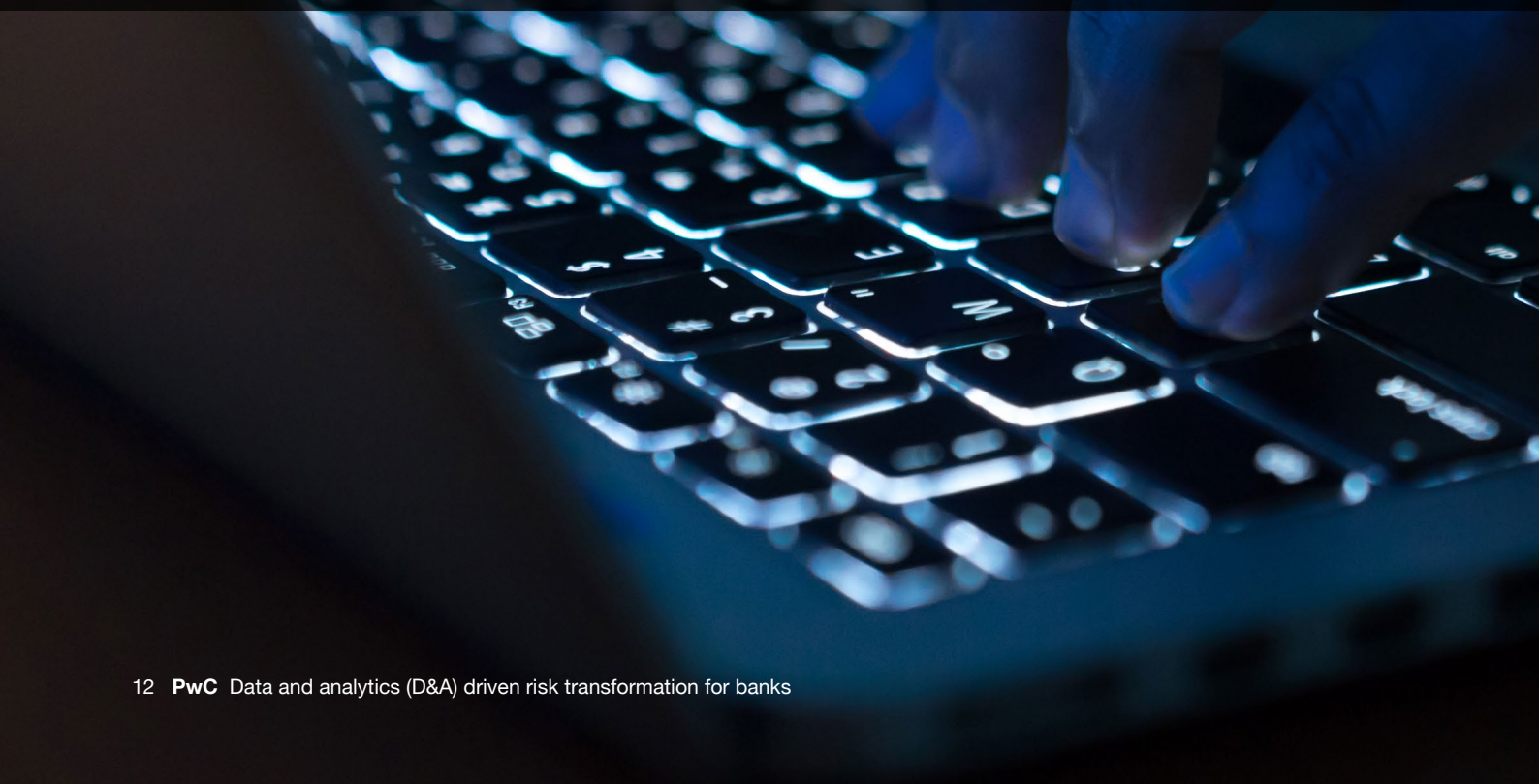
04 Better resource utilisation resulting in cost and expense optimisation

05 Legacy data and process gap identification and resolution helps in streamlining bank-wide operations and timely availability of valid, complete and accurate data

06 Increased efficiency leading to time and cost savings, and freeing up of resources

07 Enhanced operations management by reallocation of resources basis risk and regulatory insights

It is high time FS organisations embark on a D&A-driven risk transformation journey and leverage strong risk capabilities to their advantage to stay ahead in the industry.



About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 156 countries with over 295,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2022 PwC. All rights reserved.

Contact us

Mukesh Deshpande
FS Data and Analytics Leader, PwC India
mukesh.deshpande@pwc.com

Hetal Patel
Partner, PwC India
hetal.d.shah@pwc.com

Hardik Gandhi
Director, PwC India
hardik.gandhi@pwc.com

Authors

Anurag Gupta
Sushant Jadhav
Anand Raghunathan
Vaibhav Gupta

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2022 PricewaterhouseCoopers Private Limited. All rights reserved.

HS/January2022/M&C-17074